

REMARKS ON THE FOURIER COEFFICIENTS OF MODULAR FORMS

KIRTI JOSHI

ABSTRACT. We consider a variant of a question of N. Koblitz. For an elliptic curve E/\mathbb{Q} which is not \mathbb{Q} -isogenous to an elliptic curve with torsion, Koblitz has conjectured that there exists infinitely many primes p such that $N_p(E) = \#E(\mathbb{F}_p) = p+1-a_p(E)$ is also a prime. We consider a variant of this question. For a newform f , without CM, of weight $k \geq 4$, on $\Gamma_0(M)$ with trivial Nebentypus χ_0 and with integer Fourier coefficients, let $N_p(f) = \chi_0(p)p^{k-1} + 1 - a_p(f)$ (here $a_p(f)$ is the p^{th} -Fourier coefficient of f). We show under GRH and Artin's Holomorphy Conjecture that there are infinitely many p such that $N_p(f)$ has at most $[5k + 1 + \sqrt{\log(k)}]$ distinct prime factors. We give examples of about hundred forms to which our theorem applies.

To Pramodini J. Joshi,

in memoriam (1924-2009)

1. INTRODUCTION

1.1. Koblitz' question for elliptic curves. For a natural number n , let $\omega(n)$ denote the number of distinct prime factors of n and let $\Omega(n)$ be the number of primes, dividing n counted with multiplicities. Let E/\mathbb{Q} be an elliptic curve and, for a prime p of good reduction of E . Let $N_p(E) = p+1-a_p(E)$ be the number of points on the reduction of E modulo p . Assume that E is not \mathbb{Q} -isogenous to an elliptic curve with torsion. In [Kob88] the following question was studied: how often is $N_p(E)$ a prime? In [Kob88] it was conjectured that this happens infinitely often. Several authors (see [MM01, CM04, Coj05, SW05a, SW05b]) have recently studied this question.

1.2. The example of the Delta function. Motivated by this question, we study a similar problem for modular forms. Specifically, let $f(q) = \sum_{n=1}^{\infty} a_n(f)q^n$ be a cuspidal, normalized, new, Hecke eigenform on $\Gamma_0(M)$ of weight $k \geq 2$ (here $M \geq 1$ is an integer) and Nebentypus χ , without complex multiplication and with integer Fourier coefficients. Then we are interested in the number of prime factors of $N_p(f) = \chi(p)p^{k-1} + 1 - a_p(f)$. In particular one can study this for the Ramanujan modular form $\Delta(q)$ (see [Ram16]) of weight twelve

$$\Delta(q) = \sum_{n=1}^{\infty} \tau(n)q^n = q \prod_{n=1}^{\infty} (1 - q^n)^{24},$$

on $\text{SL}_2(\mathbb{Z})$. The example of Ramanujan form already shows that for a given newform the numbers $N_p(f) = \chi(p)p^{k-1} + 1 - a_p(f)$ may be composite for all primes p . Indeed

Date: Version no. delta09-arxivof October 3, 2009.

Ramanujan's congruences [Ser73] for $\tau(n)$ show that for all primes $p \geq 5$

$$(1.2.1) \quad N_p(\Delta) \equiv 0 \pmod{2^5 \cdot 3 \cdot 691},$$

so that we have $\omega(N_p(\Delta)) \geq 3$ and $\Omega(N_p(\Delta)) \geq 7$ for all $p \geq 5$; and note that $N_2(\Delta) = 2^{11} + 1 - \tau(2) = 3 \cdot 691$; $N_3(\Delta) = 3^{11} + 1 - \tau(3) = 2 \cdot 691$. So we have in any case that $\omega(N_p(\Delta)) \geq 2$, thus the obvious variant of the above question is trivially false for the Ramanujan modular form. In 9.1 we suggest a refined version of Koblitz's conjecture which includes the behavior of the sort seen for Ramanujan's Delta function.

1.3. The main question. However given a newform f of weight k on $\Gamma_0(M)$ and Nebentypus χ , with rational or integral Fourier coefficients, we may still ask if the following weaker version of Koblitz' question is still true: *do there exist infinitely many primes p such that $N_p(f) = \chi(p)p^{k-1} + 1 - a_p(f)$ has bounded number of prime factors?* In this note we will prove that this is indeed the case if we assume the Generalized Riemann Hypothesis and the generalized Riemann hypothesis. We prove the following theorems:

Theorem 1.3.1. *Assume GRH and Artin's Holomorphy Conjecture for Artin L -functions and suppose that f is a newform satisfying hypothesis 2.1. Let*

$$N_p(f) = \chi(p)p^{k-1} + 1 - a_p(f).$$

Then

- (1) *there exists infinitely many primes p such that*

$$\omega(N_p(f)) \leq [5k + 1 + \sqrt{\log(k)}],$$

- (2) *and there exists infinitely many primes p such that*

$$\Omega(N_p(f)) \leq [8k + 1 + \sqrt{\log(k)}].$$

Corollary 1.3.2. *Assume GRH and Artin's Holomorphy Conjecture for Artin L -functions. Let $\tau(n)$ be the Ramanujan τ -function. Then there are infinitely many prime p such that*

$$3 \leq \omega(p^{11} - \tau(p) + 1) \leq [61 + \sqrt{\log(12)}] = [62.57 \dots] = 62$$

and an infinity of primes p such that

$$7 \leq \Omega(N_p(\Delta)) \leq [98.57 \dots] = 98.$$

The proofs are along the lines of [SW05a, SW05b]. We use a weighted sieve to arrive at this result. We prove more precise versions of Theorems 1.3.1, Theorem 1.3.2 in Theorem 2.2.2 and Theorem 2.2.3 where we provide lower bounds for the set of such primes. These results should be compared with the known results for prime divisors of values of a fixed irreducible polynomial (see [HR74]). In Theorem 2.3.1 we provide an upper bound which is of the order of magnitude comparable to the lower bounds of Theorems 2.2.2 and Theorem 2.2.3. In section 8 we give a table of about 100 modular forms of various levels and weights where our theorem applies.

1.4. Normal order of $N_p(f)$. In contrast to the above results, in Theorem 7.1.1 we show that the average behavior of $\omega(N_p(f))$ is similar to the average behavior of $\omega(p-1)$. More precisely we show (on GRH) that $\omega(N_p(f))$ has normal order $\log \log(p)$. In fact a version of Erdos-Kac Theorem holds for $\omega(N_p(f))$. This result shows (again) that the set of primes p for which $\omega(N_p(f))$ is bounded is of zero density (on GRH).

1.5. Odds and ends. We end with some remarks about the existence of forms f for which $\omega(N_p(f)) \geq 2$ for all p . In fact we show (see Remark 9.2.1) that there exists a sequence of weights $k_i \rightarrow \infty$ as $i \rightarrow \infty$ and a normalized cusp form (but need not be eigenform) f_{k_i} of weight k_i on $\mathrm{SL}_2(\mathbb{Z})$ with integer coefficients such that $\omega(N_p(f_{k_i})) \geq 2$ for all i and for all primes $p \geq 2$. So the numbers $\omega(N_p(f)) \geq 2$ for all $p \geq 2$ for infinitely many cusp forms (normalized, but not necessarily eigenforms). In Remark 9.2.2 we record a bound for the number of primes dividing the numerator of B_n/n .

1.6. Acknowledgements. We would like to thank M. Ram Murty for his comments. We have added a refined version of Koblitz' conjecture in 9.1 in response to his question. We are grateful to the referee for many suggestions and corrections. The section 6 on the results assuming GRH (as opposed to GRH and Artin Holomorphy conjecture) was added at the referee's suggestion.

2. STATEMENT OF THE MAIN RESULTS

2.1. Hypothesis on our forms. Let $k \geq 4$ be an integer. Let

$$(2.1.1) \quad f(z) = \sum_{n=1}^{\infty} a_n(f) q^n$$

be a new, normalized, cuspidal, Hecke eigenform of weight k on $\Gamma_0(M)$ with Nebentypus χ . Following the usual convention we will simply call such a form a *newform* on $\Gamma_0(M)$ with Nebentypus χ . Throughout this paper we will assume that f does not have complex multiplication, CM for short, (see [Rib77] for definition and properties) and that f has integer Fourier coefficients, i.e., we will assume that $a_n(f) \in \mathbb{Z}$ for all $n \geq 1$. Since the field of Hecke eigenvalues contains the field of values of χ (see [Rib77]), our assumptions restrict χ to be of order at most two. Further by [Rib77, Remark 2, page 34] any form with coefficient field \mathbb{Q} and with Nebentypus of order two has CM. *So our assumption entails that f is a newform of weight $k \geq 4$ without complex multiplication on $\Gamma_0(M)$, with trivial Nebentypus χ_0 and with rational Fourier coefficients.* We will work with such forms throughout this paper. We note that if the level M is square-free, then our assumption that the form does not have complex multiplication is automatic (see [Rib77]). In section 8 we give examples of about hundred modular forms of square-free levels ≤ 21 and weights ≥ 4 where our results apply. Our list is by no means exhaustive. We note that we assume that f has weight $k \geq 4$. A form of weight two satisfying our hypothesis corresponds to elliptic curves over \mathbb{Q} (by the modularity theorem (see [Bre01, Theorem A] and references therein)) and has been covered by [MM01, CM04, Coj05, SW05a, SW05b].

A typical example of a form which satisfies the above hypothesis and of particular interest to us is the Ramanujan cusp form of weight twelve given by

$$(2.1.2) \quad \Delta(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n.$$

The unique normalized cuspidal eigen forms Δ_k , of weights k for $k = 12, 16, 18, 20, 22, 26$ (with $\Delta_{12} = \Delta$) on $\mathrm{SL}_2(\mathbb{Z})$ are also forms which satisfy our hypothesis.

By the results of Deligne ([Del69]) we have for $f(z)$ satisfying our hypothesis and for all prime $p \nmid M$, that

$$(2.1.3) \quad |a_p(f)| \leq 2p^{(k-1)/2},$$

and in particular for the Ramanujan modular form (2.1.2), the famous assertion of Ramanujan:

$$(2.1.4) \quad |\tau(p)| \leq 2p^{(11)/2}.$$

2.2. The main result. For a form f as in 2.1, we write

$$(2.2.1) \quad L(f, s) = \sum_{n=1}^{\infty} \frac{a_n(f)}{n^s}.$$

Then by [Del69] we know that $L(f, s)$ converges for $\mathrm{Re}(s) > \frac{k-1}{2} + 1$ and has an analytic continuation to a holomorphic function to all of \mathbb{C} . We now state the more precise forms of the theorems stated in the introduction, which we will prove in the subsequent subsections.

Theorem 2.2.2. *Assume GRH and Artin's Holomorphy Conjecture for Artin L -functions and suppose that f is a newform satisfying hypothesis 2.1.*

- (1) *There exists a positive constant $c_1(f)$ depending on f such that for $X \gg 0$, one has*

$$\# \left\{ p \leq X : \omega(N_p(f)) \leq [5k + 1 + \sqrt{\log(k)}] \right\} \geq c_1(f) \frac{X}{\log(X)^2}$$

- (2) *There exists a positive constant $c_2(f)$ depending on f such that for X sufficiently large, one has*

$$\# \left\{ p \leq X : \Omega(N_p(f)) \leq [8k + 1 + \sqrt{\log(k)}] \right\} \geq c_2(f) \frac{X}{\log(X)^2}$$

Corollary 2.2.3. *Assume GRH and Artin's Holomorphy Conjecture for Artin L -functions. Let $\Delta(q) = \sum_{n=1}^{\infty} \tau(n) q^n$ be the Ramanujan cusp form on $\mathrm{SL}_2(\mathbb{Z})$ of weight 12. Let X be sufficiently large. Then*

- (1) *there exists a positive constant $c_1(\Delta)$ depending on Δ such that for $X \gg 0$ one has*

$$\# \left\{ p \leq X : \omega(p^{11} + 1 - \tau(p)) \leq 62 \right\} \geq c_1(\Delta) \frac{X}{\log(X)^2}$$

- (2) *there exists a positive constant $c_2(\Delta)$ depending on Δ such that for $X \gg 0$ one has*

$$\# \left\{ p \leq X : \Omega(p^{11} + 1 - \tau(p)) \leq 98 \right\} \geq c_2(\Delta) \frac{X}{\log(X)^2}$$

Corollary 2.2.3 is, of course, immediate from Theorem 2.2.2.

2.3. Upper bound. We will also prove the following upper bound which shows that the lower bounds of Theorem 2.2.2 are of the right order of magnitude, though a precise asymptotic formula seems out of reach at the moment (even under GRH and Artin's Holomorphy Conjecture).

Theorem 2.3.1. *Let $f(q) = \sum_{n=1}^{\infty} a_n(f)q^n$ be a newform satisfying the hypothesis 2.1. Assume GRH and Artin's Holomorphy Conjecture for Artin L -functions. Then we have*

$$\#\{p \leq X : \Omega(N_p(f)) \leq 9k - 8\} \ll \frac{X}{(\log X)^2}.$$

3. NUTS AND BOLTS

3.1. Let $f(q) = \sum_{n=1}^{\infty} a_n(f)q^n$ be a newform satisfying our hypothesis 2.1. Let us write

$$(3.1.1) \quad N_p(f) = \chi(p)p^{k-1} - a_p(f) + 1$$

Then by the theory of Hecke operators (for p not dividing the level) we know that $N_p(f)$ is the value at $Y = 1$ of the characteristic polynomial $Y^2 - a_p(f)Y + \chi(p)p^{k-1}$ of the Hecke operator T_p .

Write $Y^2 - a_p(f)Y + \chi(p)p^{k-1} = (Y - \alpha_p(f))(Y - \beta_p(f))$. Then we know by [Del69] that $|\alpha_p(f)| = |\beta_p(f)| = p^{(k-1)/2}$

3.2. By the work of Deligne (and Deligne-Serre for weight one forms) [Del69] we know that for every prime ℓ , associated to f (as in 2.1) we have an ℓ -adic Galois representation

$$(3.2.1) \quad \rho_{f,\ell} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{Q}_\ell)$$

such that for every prime $p \nmid M\ell$, we have

$$(3.2.2) \quad \text{Tr}(\rho_{f,\ell}(\text{Frob}_p)) = a_p(f)$$

$$(3.2.3) \quad \det(\rho_{f,\ell}(\text{Frob}_p)) = \chi(p)p^{k-1}.$$

3.3. Following Serre, Swinnerton-Dyer and Ribet (see [Ser69, Ser73, Rib77, Rib85]) we may also consider the corresponding “mod ℓ ” representations. We recall the following theorem from [Ser73, Rib85].

Theorem 3.3.1. *Let f be a modular form as in 2.1. Let*

$$\bar{\rho}_{f,\ell} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{F}_\ell)$$

be the mod ℓ Galois representation associated to f . Then there exists an integer m_f depending on f , such that for all ℓ not dividing m_f , we have

$$\text{Image}(\bar{\rho}_{f,\ell}) = G_\ell,$$

where

$$G_\ell = \{g \in \text{GL}_2(\mathbb{F}_\ell) : \det(g) \in (\mathbb{F}_\ell^*)^{(k-1)}\}.$$

3.4. Let $K_{f,\ell} = \bar{\mathbb{Q}}^{\ker(\bar{\rho}_{f,\ell})}$. Then $K_{f,\ell}$ is the fixed field of $\ker(\bar{\rho}_{f,\ell})$ and the extension $K_{f,\ell}$ is Galois with Galois group

$$(3.4.1) \quad \text{Gal}(K_{f,\ell}/\mathbb{Q}) \simeq G_\ell.$$

3.5. More generally, let $\bar{\rho}_{f,\ell^n} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{Z}/\ell^n)$ be the mod ℓ^n Galois representation associated to f . Let $K_{f,\ell^n} = \bar{\mathbb{Q}}^{\ker(\bar{\rho}_{f,\ell^n})}$ be the fixed field of the kernel of ρ_{f,ℓ^n} . Then K_{f,ℓ^n} is Galois with Galois group contained in $\text{GL}_2(\mathbb{Z}/\ell^n)$.

Proposition 3.5.1. *Let f be as in 2.1. Then the following are equivalent:*

- (1) $\ell^n | N_p(f)$,
- (2) *either $\bar{\rho}_{f,\ell^n}(\text{Frob}_p)$ has an eigenvalue equal to 1, or $\bar{\rho}_{f,\ell^t}(\text{Frob}_p)$ is unipotent for some $1 \leq t < n$.*

Proof. Since $\ell^n | N_p(f)$ if and only if $\ell^n | (p^{k-1} - a_p(f) + 1)$, so $\ell^n | (1 - \alpha_p(f))(1 - \beta_p(f))$ where $Y^2 - a_p(f)Y + p^{k-1} = (Y - \alpha_p(f))(Y - \beta_p(f))$. Hence if neither of $\alpha_p(f) - 1, \beta_p(f) - 1$ are divisible by ℓ^n , then $\alpha_p(f) \equiv 1 \pmod{\ell^r}$ and $\beta_p(f) \equiv 1 \pmod{\ell^s}$, for some $1 \leq r, s < n$ and $r + s = n$. So that both $\alpha_p(f) \equiv \beta_p(f) \equiv 1 \pmod{\ell^t}$ with $t = \min(r, s)$. So this says that $\bar{\rho}_{f,\ell^n}(\text{Frob}_p)$ acts as a unipotent matrix modulo a suitable power, say ℓ^t with $1 \leq t < n$, of ℓ . This proves the theorem. \square

Lemma 3.5.2. *Let $C_{\ell,n} \subset \text{GL}_2(\mathbb{Z}/\ell^n)$ be the subset of matrices $g \in \text{GL}_2(\mathbb{Z}/\ell^n)$ such that g either has an eigenvalue 1 or for some $1 \leq t < n$, the image of g under the natural map $\text{GL}_2(\mathbb{Z}/\ell^n) \rightarrow \text{GL}_2(\mathbb{Z}/\ell^t)$, is identity. Then $C_{\ell,n}$ is a conjugacy set (i.e. a union of conjugacy classes of $\text{GL}_2(\mathbb{Z}/\ell^n)$).*

Proof. This is clear. \square

3.6. We will use the following lemma.

Lemma 3.6.1. *Let $\lambda = \gcd(k-1, \ell-1)$. Then*

$$\#C_{\ell,1} = \frac{\ell^3 - (\lambda+1)\ell}{\lambda}.$$

Proof. We count using method of [Was86]. By definition $\#C_{\ell,1}$ is the number of matrices in G_ℓ which have at least one eigenvalue one. The number of such matrices is the number of matrices which look like

$$\begin{pmatrix} 1 & * \\ 0 & u^\lambda \end{pmatrix}$$

where $u \in \mathbb{F}_\ell^*$ times the number of one dimensional subspaces of $\mathbb{F}_\ell \oplus \mathbb{F}_\ell$ minus the number of matrices which get counted twice; the former number is $\ell(\ell-1)/\lambda$ times $(\ell+1)$; while the number of matrices which get counted twice are the ones with both the eigenvalues equal to one (and this number is ℓ). So the number of matrices in $C_{\ell,1}$ is $(\ell+1)\ell(\ell-1)/\lambda - \ell$. This easily simplifies to $\frac{\ell^3 - (\lambda+1)\ell}{\lambda}$. \square

Lemma 3.6.2. *We have*

$$\#G_\ell = \frac{(\ell^2 - 1)(\ell^2 - \ell)}{\lambda}.$$

Proof. This is clear from the exact sequence

$$1 \rightarrow \text{SL}_2(\mathbb{F}_\ell) \rightarrow G_\ell \rightarrow (\mathbb{F}_\ell^*)^\lambda \rightarrow 1,$$

and the standard formula for computing the order of $\text{SL}_2(\mathbb{F}_\ell)$. This proves the assertion. \square

Lemma 3.6.3. *For $\ell \gg 0$, and $\lambda = \gcd(k-1, \ell-1)$ we have*

$$\frac{\#C_{\ell,1}}{G_\ell} = \frac{1}{\ell} + O\left(\frac{1}{\ell^3}\right).$$

Proof. Clear from the fact that

$$\frac{\#C_{\ell,1}}{G_\ell} = \frac{\frac{1}{\ell} - \frac{\lambda+1}{\ell^3}}{1 - \frac{1}{\ell} - \frac{1}{\ell^2} + \frac{1}{\ell^4}},$$

and so the assertion follows for $\ell \gg 0$ by expansion of the denominator. \square

4. THE WEIGHTED SIEVE

4.1. We will prove Theorem 2.2.2 by using a suitable weighted sieve due to Richert [HR74]. The sieve problem we encounter here is a one dimensional sieve problem in the parlance of “sieve methods” and we will use notations from [HR74] in this section. We begin with the notations and conventions we need to apply the results of [HR74, Theorem 9.1, Lemma 9.1].

4.2. Let \mathcal{A} be a finite set of integers (need not be positive or distinct). Let \mathcal{P} be an infinite set of prime numbers. For each prime $\ell \in \mathcal{P}$, let $\mathcal{A}_\ell = \{a \in \mathcal{A} : a \equiv 0 \pmod{\ell}\}$. We write

$$\#\mathcal{A} = X + R_1$$

and

$$\#\mathcal{A}_\ell = \delta(\ell)X + R_\ell$$

where X is some approximation to \mathcal{A} , and $\delta(\ell)X$ is some approximation to \mathcal{A}_ℓ . For a square-free positive integer d composed of primes of \mathcal{P} , let

$$(4.2.1) \quad \delta(d) = \prod_{\ell|d} \delta(\ell)$$

$$(4.2.2) \quad \mathcal{A}_d = \bigcap_{\ell|d} \mathcal{A}_\ell$$

$$(4.2.3) \quad R_d = \#\mathcal{A} - \delta(d)X.$$

For $z > 0$, let

$$P(z) = \prod_{\ell \in \mathcal{P}, \ell < z} \ell,$$

$$W(z) = \prod_{\ell \in \mathcal{P}, \ell < z} (1 - \delta(\ell)).$$

4.3. **Sieving hypotheses.** We will assume that these satisfy the following hypothesis

(Ω_1): there exists a constant $A_1 \geq 0$ such that $0 \leq \delta(\ell) \leq 1 - 1/A_1$ for all $\ell \in \mathcal{P}$.

($\Omega_2(1, L)$): there exists a constant $L \geq 1$ and A_2 such that if $2 \leq w \leq z$, then

$$-L \leq \sum_{2 \leq w \leq z} \delta(\ell) \log \ell - \log(z/w) \leq A_2,$$

($R(1, \alpha)$): there exists $0 < \alpha < 1$ and $A_3, A_4 \geq 1$ such that, if $X \geq 2$ then

$$\sum_{d < X^\alpha / (\log(X))^{A_3}} \mu(d)^2 3^{\omega(d)} |R_d| \leq A_4 \frac{X}{(\log X)^2}$$

4.4. The sifting function. With \mathcal{A}, \mathcal{P} as above, we consider a weighted sifting function of the following form

$$(4.4.1) \quad \mathcal{W}(\mathcal{A}, \mathcal{P}, v, u, \lambda) = \sum_{a \in \mathcal{A}, (a, P(X^{1/v})=1)} \left(1 - \sum_{X^{1/v} \leq p < X^{1/u}, p|a, p \in \mathcal{P}} \beta(p, \lambda) \right),$$

where

$$(4.4.2) \quad \beta(p, \lambda) = \begin{cases} \lambda \left(1 - u \frac{\log p}{\log X} \right) & \text{if } X^{1/v} \leq p < X^{1/u}, p \in \mathcal{P} \\ 0 & \text{otherwise.} \end{cases}$$

4.5. We recall the following form of Richert's weighted one dimensional sieve from [HR74, Theorem 9.1, Lemma 9.1].

Theorem 4.5.1. *Let the notations and conventions be as in 4.2, 4.3. Assume that hypothesis Ω_1 , $\Omega_2(1, L)$ and $R(1, \alpha)$ hold for a set \mathcal{A} as in 4.2, 4.3. Suppose further that there exists $u, v, \lambda \in \mathbb{R}$ and $A_5 \geq 1$ such that*

$$\frac{1}{\alpha} < u < v, \frac{2}{\alpha} \leq v \leq \frac{4}{\alpha}, 0 < \lambda < A_5.$$

Then

$$\mathcal{W}(\mathcal{A}, \mathcal{P}, u, v, \lambda) \geq XW(X^{1/v}) \left(F(\alpha, v, u, \lambda) - \frac{cL}{(\log X)^{1/14}} \right),$$

where

$$F(\alpha, v, u, \lambda) = \frac{2e^\gamma}{\alpha v} \left(\log(\alpha v - 1) - \lambda \alpha u \log \frac{v}{u} + \lambda(\alpha u - 1) \log \frac{\alpha v - 1}{\alpha u - 1} \right).$$

Here γ is Euler's constant.

4.6. Proofs of the main theorems. We will now apply the Theorem 4.5.1 to the following situation. We will take

$$\mathcal{A} = \{N_p(f) : p \leq X\},$$

and

$$\mathcal{P} = \{p : p \text{ a prime}\},$$

so that $\#\mathcal{A} = \pi(X)$ and by the prime number theorem, we may write $\#\mathcal{A} = \#\mathcal{A}_1 = \frac{X}{\log(X)} + R_1$. By the Chebotarev density theorem applied to the extensions $K_{\ell, f}$, we may take $\delta(\ell) \frac{X}{\log(X)}$ as an approximation to $\#\mathcal{A}_\ell$, where $\delta(\ell) = \frac{\#C_{\ell, 1}}{\#G_\ell}$ (see 3.6.3). To get uniform error term in the Chebotarev density theorem for the extensions K_ℓ valid for a range of ℓ we will need GRH and Artin's Holomorphy Conjecture (especially the version of Chebotarev density theorem of [MMS88]). To apply Theorem 4.5.1 we have to verify that the hypothesis $\Omega_1, \Omega_2(1, L)$, and $R(1, \alpha)$ hold (see 4.3). We will do this now.

Lemma 4.6.1. *The hypothesis (Ω_1) holds with a suitable $A_1 > 0$, i.e., we have*

$$0 \leq \delta(\ell) \leq 1 - \frac{1}{A_1},$$

with a suitable A_1 .

Proof. This is clear from the fact that $\delta(\ell) = \frac{\#C_{\ell, 1}}{\#G_\ell} = \frac{1}{\ell} + O(\frac{1}{\ell^3})$ (see Lemma 3.6.3). \square

Lemma 4.6.2. *The hypothesis $(\Omega_2(1, L))$ holds with a suitable L , i.e., there exists an $A_2 \geq 1$ and an L such that for $2 \leq w \leq z$, we have*

$$-L \leq \sum_{w \leq p < z} \delta(\ell) \log(\ell) - \log \frac{z}{w} \leq A_2$$

Proof. This is again clear from Lemma 3.6.3 and Mertens's Theorem (see [HW79, page 351]). Indeed $\delta(\ell) = \frac{1}{\ell} + O(\frac{1}{\ell^3})$. \square

The next step is to establish that $R(1, \alpha)$ holds. This is where we use GRH and Artin's Holomorphy Conjecture. To prove $R(1, \alpha)$ holds we need a form of Chebotarev density theorem currently available under GRH and Artin's Holomorphy Conjecture (see [MMS88]).

Lemma 4.6.3. *Let f be a newform satisfying our hypothesis 2.1. Let*

$$R_d = \pi_f(X, d) - \delta(d) Li(X).$$

Assume GRH and Artin's Holomorphy Conjecture for all Artin L -functions. Then hypothesis $(R(1, \alpha))$ holds with any $\alpha < 1/5$, i.e., we have for any $\alpha < 1/5$:

$$\sum_{d < X^\alpha / (\log(X))^B} \mu(d)^2 3^{\omega(d)} |R_d| \ll \frac{X}{(\log X)^2}$$

Proof. Observe that we have from [HW79, page 260], that

$$3^{\omega(n)} \leq d(n)^{3 \log 3 / \log 2} \ll n^\varepsilon.$$

Thus we have

$$\sum_{d < X^\alpha / (\log X)^B} \mu^2(d) 3^{\omega(d)} |R_d| \ll \sum_{d < X^\alpha / (\log X)^B} d^\varepsilon |R_d|.$$

Assuming GRH and Artin's Holomorphy Conjecture and by [MMS88] we have

$$|R_d| = O(d^{3/2} X^{1/2} \log(dX)).$$

So the sum in question is certainly

$$\ll \sum_{d < X^\alpha / (\log(X))^B} d^{3/2+\varepsilon} X^{1/2} \log(dX),$$

which is

$$\ll X^{1/2} \log(X) \sum_{d < X^\alpha / (\log X)^B} d^{3/2+\varepsilon},$$

and this is, by partial summation,

$$\ll X^{1/2+(5/2)\alpha+\varepsilon}.$$

For $\alpha < 1/5$, the sum in the assertion is

$$\ll X^{1/4+\varepsilon}$$

and clearly this is certainly $\ll \frac{X}{(\log X)^2}$. This proves the assertion. \square

Lemma 4.6.4. *For $X \gg 0$, we have*

$$W(X) \gg \frac{1}{\log X}$$

Proof. This is clear from our estimates for $\delta(\ell)$ and Mertens's Theorem [HW79, page 351] \square

4.7. Choice of sieve parameters. Thus we can apply Theorem 4.5.1 to our situation and we will make this explicit now. To apply Theorem 4.5.1 we need to choose α, u, v, λ satisfying conditions of the theorem.

We choose as follows. We will take $k \geq 3$ and:

$$(4.7.1) \quad \alpha = \frac{1}{5} - \frac{1}{5k} = \frac{k-1}{5k},$$

$$(4.7.2) \quad u = \frac{5k}{k-1} + \frac{1}{k-1} = \frac{5k+1}{k-1}$$

$$(4.7.3) \quad v = \frac{4}{\alpha} = \frac{20k}{k-1},$$

$$(4.7.4) \quad \lambda = \frac{1}{\sqrt{\log(k)}}.$$

Then we have

$$\frac{1}{\alpha} = \frac{5k}{k-1} < u = \frac{5k+1}{k-1} < v = \frac{4}{\alpha} = \frac{20k}{k-1}.$$

With these choices, we define

$$G_1(k) = F\left(\frac{k-1}{5k}, \frac{20k}{k-1}, \frac{5k+1}{k-1}, \frac{1}{\sqrt{\log(k)}}\right)$$

explicitly this is given by

$$(4.7.5) \quad G_1(k) = \frac{e^\gamma \left(5k \log(3) \sqrt{\log(k)} + \log(15k) - (1+5k) \log(20k/1+5k)\right)}{10k \sqrt{\log(k)}}.$$

It is clear that for $k \gg 0$, one has $G_1(k) > 0$ and numerically one checks that for all $k \geq 3.039 \dots$, we have $G_1(k) > 0$. Thus we have that $F(\alpha, v, u, \lambda) > 0$ for these choices of the parameters. So we can apply Theorem 4.5.1, and note that by the prime number theorem (or by Chebyshev's Theorem) we have $\#\mathcal{A} \gg \frac{X}{\log X}$ and so we deduce that

$$\mathcal{W}(\mathcal{A}, \mathcal{P}, u, v, \lambda) \gg \frac{X}{(\log X)^2}.$$

Now suppose that p is such that N_p has positive weight in the sum $\mathcal{W}(\mathcal{A}, \mathcal{P}, u, v, \lambda)$ then we claim that $\omega(N_p(f)) \leq [5k + \sqrt{\log(k)}]$. This will prove our theorem. Indeed as the sum is positive for the above choices of parameters, and so there are primes $p \leq X$ where $N_p(f)$ has this property.

Now observe that for any such p , the “weight” it contributes is positive so

$$(4.7.6) \quad 0 < \mathbf{w}(p) = 1 - \lambda \left(\sum_{X^{1/v} < q < X^{1/u}, q|N_p(f)} \left(1 - u \frac{\log(q)}{\log(X)}\right) \right),$$

and $N_p(f)$ has no prime divisors $q \leq X^{1/v}$; moreover any prime divisor q of $N_p(f)$ with $q \geq X^{1/u}$ we have

$$1 - u \frac{\log(q)}{\log(X)} \leq 0,$$

and so even if we include the contribution of primes $q > X^{1/u}$, in the sum (4.7.6) we see that

$$0 < 1 - \lambda \left(\sum_{q|N_p(f)} \left(1 - u \frac{\log(q)}{\log(X)} \right) \right),$$

and this gives

$$(4.7.7) \quad \omega(N_p(f)) = \sum_{q|N_p(f)} 1 < u \sum_{q|N_p(f)} \frac{\log(q)}{\log(X)} + \frac{1}{\lambda}$$

$$(4.7.8) \quad = u \frac{\log(N_p(f))}{\log(X)} + \frac{1}{\lambda}$$

$$(4.7.9)$$

Now we use the Deligne-Ramanujan-Weil estimate:

$$N_p(f) = p^{k-1} + 1 - a_p(f) \leq p^{k-1} + 1 + 2p^{(k-1)/2},$$

and we deduce that for sufficiently large X we have

$$\sum_{q|N_p(f)} \frac{\log(q)}{\log(X)} \leq \frac{\log(N_p(f))}{\log(X)}$$

By the Deligne-Ramanujan-Weil estimate the last term is bounded by $\frac{\log(X^{k-1}+1+2X^{(k-1)/2})}{\log(X)}$ and this is

$$\leq k - 1 + \frac{\log(1 - X^{-(k-1)} + 2X^{-(k-1)/2})}{\log(X)}$$

For any $\varepsilon > 0$, we can find $X \geq X_0(k, \varepsilon)$ such that the second term in the above is less than $\varepsilon \frac{(k-1)}{(5k+1)}$. So we have

$$\omega(N_p(f)) \leq u \left((k-1) + \varepsilon \frac{k-1}{5k+1} \right) + \frac{1}{\lambda},$$

and now our assertion follows using the fact that we have chosen

$$u = \frac{(5k+1)}{k-1}, \lambda = \frac{1}{\sqrt{\log(k)}}.$$

Thus

$$\omega(N_p(f)) \leq 5k + 1 + \sqrt{\log(k)} + \varepsilon.$$

For a fixed k and X suitably large, we may choose $\varepsilon > 0$ so small that

$$[5k + 1 + \sqrt{\log(k)} + \varepsilon] = [5k + 1 + \sqrt{\log(k)}]$$

and so the first assertion follows.

To prove the second assertion, we observe that we need to estimate the number of primes $p \leq X$ which contribute to the sifting function with positive weights and have a prime divisor $\ell | N_p(f)$ with $\ell^2 | N_p(f)$ and $X^{1/v} \leq \ell \leq X^{1/u}$. We will follow the argument of [SW05a, SW05b] to do this. We easily estimate the number of elements of $C_{\ell,2}$ to as indicated in [SW05a, SW05b] and obtain

$$\frac{\#C_{\ell,2}}{\#G_\ell} = \frac{1}{\ell^2} + O(\ell^{-3}).$$

Thus we have

$$\begin{aligned}
\#\{p \leq X : \ell^2 | N_p(f), X^{1/v} \leq \ell \leq X^{1/u}\} &= \sum_{X^{1/v} \leq \ell \leq X^{1/u}} \#\{p \leq X : \ell^2 | N_p(f)\}. \\
&\ll \frac{X}{\log(X)} \sum_{X^{1/v} \leq \ell \leq X^{1/u}} \frac{1}{\ell^2} + X^{1/2+\varepsilon} \sum_{X^{1/v} \leq \ell \leq X^{1/u}} \ell^3 \\
&= o\left(\frac{X}{\log(X)^2}\right),
\end{aligned}$$

provided $u > 8$. So we choose a new set of u, v, λ as follows:

$$(4.7.10) \quad \alpha = \frac{k-1}{5k},$$

$$(4.7.11) \quad u = \frac{8k+1}{k-1},$$

$$(4.7.12) \quad v = \frac{16k}{k-1},$$

$$(4.7.13) \quad \lambda = \frac{1}{\sqrt{\log(k)}}.$$

Then we see that

$$G_2(k) = F\left(\frac{k-1}{5k}, \frac{16k}{k-1}, \frac{8k+1}{k-1}, \frac{1}{\sqrt{\log(k)}}\right).$$

Explicitly we have

$$G_2(k) = \frac{e^\gamma}{16k\sqrt{\log(k)}} \left\{ 5 \log(11/5)k\sqrt{\log(k)} + (3k+1) \log\left(\frac{11k}{3k+1}\right) - (8k+1) \log\left(\frac{16k}{8k+1}\right) \right\}$$

and it is easy to see that $G_2(k) > 0$ for $k \gg 0$ and numerically one has $G_2(k)$ is positive for $k \geq 4$.

Thus for these choices of u, v, λ the primes $p \leq X$ such that $N_p(f)$ has a small square divisor do not contribute to the lower bound for the sifting function. Let p be such a prime, so that $N_p(f)$ makes a positive contribution to the sum \mathscr{W} . Then for such a p , N_p does not have any prime divisors less than $X^{1/v}$, and for primes $\ell | N_p(f)$ such that $X^{1/v} < \ell < X^{1/u}$, ℓ^2 does not divide $N_p(f)$, while for the primes $\ell > X^{1/u}$ which divide $N_p(f)$ (possibly dividing several times) the contribution to \mathscr{W} is always positive. So we may replace, in our previous argument, the function $\omega(N_p(f))$ by $\Omega(N_p(f))$. Indeed we have

$$0 < \mathbf{w}(p) < 1 - \lambda \left(\sum_{q^m | N_p(f)} \left(1 - u \frac{\log(q)}{\log(X)} \right) \right),$$

and this gives

$$(4.7.14) \quad \Omega(N_p(f)) = \sum_{q^m | N_p(f)} 1 < u \sum_{q^m | N_p(f)} \frac{\log(q)}{\log(X)} + \frac{1}{\lambda}$$

$$(4.7.15) \quad = u \frac{\log(N_p(f))}{\log(X)} + \frac{1}{\lambda}$$

$$(4.7.16)$$

Now we use the Deligne-Ramanujan-Weil estimate (note that $\chi(p) = 1$ for all but finite number of primes as χ is trivial):

$$N_p(f) = \chi(p)p^{k-1} + 1 - a_p(f) \leq p^{k-1} + 1 + 2p^{(k-1)/2},$$

and we deduce that for sufficiently large X we have

$$\sum_{q|N_p(f)} \frac{\log(q)}{\log(X)} \leq \frac{\log(N_p(f))}{\log(X)}$$

By the Weil estimate the last term is bounded by $\frac{\log(X^{k-1} + 1 + 2X^{(k-1)/2})}{\log(X)}$ and this is

$$\leq k - 1 + \frac{\log(1 - X^{-(k-1)} + 2X^{-(k-1)/2})}{\log(X)}$$

For any $\varepsilon > 0$, we can find $X \geq X_0(k, \varepsilon)$ such that the second term in the above is less than $\varepsilon \frac{(k-1)}{(5k+1)}$. So we have

$$\Omega(N_p(f)) \leq u \left((k-1) + \varepsilon \frac{k-1}{5k+1} \right) + \frac{1}{\lambda},$$

and now our assertion follows using the fact that we have chosen

$$u = \frac{(8k+1)}{k-1}, \lambda = \frac{1}{\sqrt{\log(k)}}.$$

Thus

$$\Omega(N_p(f)) \leq 8k + 1 + \sqrt{\log(k)} + \varepsilon.$$

For a fixed k and X suitably large, we may choose $\varepsilon > 0$ so small that

$$[8k + 1 + \sqrt{\log(k)} + \varepsilon] = [8k + 1 + \sqrt{\log(k)}]$$

and so the first assertion follows. Thus we see that

$$\# \left\{ p \leq X : \Omega(N_p(f)) \leq 8k + 1 + \sqrt{\log(k)} \right\} \gg \mathcal{W}(\mathcal{A}, \mathcal{P}, v, u, \lambda) \gg c_2(f) \frac{X}{\log(X)^2}.$$

This proves our assertion.

4.8. Now we can prove the corollary. For the Ramanujan modular form

$$\Delta(q) = \sum_{n=1}^{\infty} \tau(n)q^n$$

we have $k = 12$ and hence we deduce assuming GRH and Artin's Holomorphy Conjecture for Artin L -functions that, there exists infinitely many prime p

$$3 \leq \omega(p^{11} + 1 - \tau(p)) \leq [61 + \sqrt{\log(12)}] = 62.$$

So on GRH and Artin's Holomorphy Conjecture, there exists infinitely many primes p , such that $p^{11} + 1 - \tau(p)$ has at most $[61 + \sqrt{\log(12)}] = 62$ prime factors. Moreover there also exists infinite many primes p such that

$$7 \leq \Omega(p^{11} + 1 - \tau(p)) \leq [97 + \sqrt{\log(12)}] = 98.$$

As indicated in the introduction, the bounds $\omega(N_p(\Delta)) \geq 3$ and $\Omega(N_p(\Delta)) \geq 7$ are consequences of the Ramanujan congruences for $\Delta(q)$. This completes the proof of Theorem 2.2.3.

5. UPPER BOUNDS

5.1. We can also obtain an upper bound (again under GRH and Artin's Holomorphy Conjecture) which shows that the lower bounds are of the right order of magnitude. The upper bound is obtained using Selberg's sieve.

Theorem 5.1.1. *Let $f(q) = \sum_{n=1}^{\infty} a_n(f)q^n$ be a newform satisfying hypothesis 2.1. Assume GRH and Artin's Holomorphy Conjecture for Artin L-functions. Then we have*

$$\#\{p \leq X : \Omega(N_p(f)) \leq 9k - 8\} \ll \frac{X}{(\log X)^2}.$$

Proof. Let $\mathcal{A} = \{N_p(f) : p \leq X\}$, \mathcal{P} be the set of all primes. Let $P(z) = \prod_{p < z, p \in \mathcal{P}} p$; and let

$$\mathcal{S}(\mathcal{A}, \mathcal{P}, z) = \sum_{a \in \mathcal{A}, (a, P(z))=1} 1.$$

Then [HR74, Theorem 5.1, Chapter 5] provides a convenient way for estimating $\mathcal{S}(\mathcal{A}, \mathcal{P}, z)$ under the hypothesis $(\Omega_1), (\Omega_2(1, L))$ (see 4.3). Since we have already verified that these hypothesis hold in our setup, we can proceed to apply the [HR74, Theorem 5.1, Chapter 5] with $z = X^{1/9}$ and we obtain

$$\mathcal{S}(\mathcal{A}, \mathcal{P}, X^{1/9}) \ll \frac{X}{(\log X)^2}.$$

Let $p \leq X$ be a prime such that $N_p(f)$ contributes to the sum $\mathcal{S}(\mathcal{A}, \mathcal{P}, X^{1/9})$, then for any prime $\ell | N_p(f)$, we have $\ell > X^{1/9}$. So that we see that

$$N_p(f) > X^{\Omega(N_p(f))/9}.$$

On the other hand, for $p \leq X$, and $X \gg 0$, we have $N_p(X) \leq 2X^{k-1}$, so that we have

$$X^{\Omega(N_p(f))/9} < N_p(f) < 2X^{k-1},$$

from which we see that one certainly has $\Omega(N_p(f)) \leq 9(k-1) + 1$. This proves the theorem. \square

6. RESULTS ON GRH

6.1. We indicate briefly, the results one can obtain on GRH (as opposed to GRH and Artin Holomorphy conjecture). As one might expect the results are weaker than the ones obtained in the preceding sections. The main ingredient of the proof which is influenced by GRH or GRH and Artin Holomorphy conjecture is the Chebotarev density theorem of [MMS88]. On GRH the error terms in the Chebotarev density theorem are weaker and the bounds on $\omega(N_p(f))$ and $\Omega(N_p(f))$ are correspondingly weaker. Both sets of hypothesis do however imply the existence of infinitely many primes where $\Omega(N_p(f))$ (and hence $\omega(N_p(f))$) is bounded by a constant depending on the weight of f . To keep the discussion brief we will prove the result for $\omega(N_p(f))$.

Theorem 6.1.1. *Assume GRH for Artin L-functions and suppose that f is a newform satisfying hypothesis 2.1. Then there exists a positive constant $c_1(f)$ depending on f such that for $X \gg 0$, one has*

$$\#\left\{p \leq X : \omega(N_p(f)) \leq [8k + 1 + \sqrt{\log(k)}]\right\} \geq c_1(f) \frac{X}{\log(X)^2}.$$

Corollary 6.1.2. *Assume GRH for Artin L-functions. Let $\Delta(q) = \sum_{n=1}^{\infty} \tau(n)q^n$ be the Ramanujan cusp form on $\mathrm{SL}_2(\mathbb{Z})$ of weight 12. Let X be sufficiently large. Then there exists a positive constant $c_1(\Delta)$ depending on Δ such that for $X \gg 0$ one has*

$$\#\{p \leq X : \omega(p^{11} + 1 - \tau(p)) \leq 98\} \geq c_1(\Delta) \frac{X}{\log(X)^2}.$$

Proof. The proofs of Theorem 6.1.1 and Corollary 6.1.1 are similar to the proofs of Theorem 2.2.2 and Corollary 1.3.2. So we will indicate the changes required in the argument and the choice of the sieving parameters we make which allows us to arrive at the stated results. The change in our hypothesis from Artin Holomorphy and GRH to GRH alone changes the error term in the Chebotarev density theorem (see [MMS88]). The change affects Lemma 4.6.3 which we replace by the following Lemma 6.1.3 given below. \square

Lemma 6.1.3. *Let f be a newform satisfying our hypothesis 2.1. Let*

$$R_d = \pi_f(X, d) - \delta(d) \mathrm{Li}(X).$$

Assume GRH for all Artin L-functions. Then hypothesis $(R(1, \alpha))$ holds with any $\alpha < 1/8$, i.e., we have for any $\alpha < 1/8$:

$$\sum_{d < X^\alpha / (\log(X))^B} \mu(d)^2 3^{\omega(d)} |R_d| \ll \frac{X}{(\log X)^2}$$

Proof. Observe that we have from [HW79, page 260], that

$$3^{\omega(n)} \leq d(n)^{3 \log 3 / \log 2} \ll n^\varepsilon.$$

Thus we have

$$\sum_{d < X^\alpha / (\log X)^B} \mu^2(d) 3^{\omega(d)} |R_d| \ll \sum_{d < X^\alpha / (\log X)^B} d^\varepsilon |R_d|.$$

Assuming GRH by [MMS88] we have

$$|R_d| = O(d^3 X^{1/2} \log(dX)).$$

So the sum in question is certainly

$$\ll \sum_{d < X^\alpha / (\log(X))^B} d^{3+\varepsilon} X^{1/2} \log(dX),$$

which is

$$\ll X^{1/2} \log(X) \sum_{d < X^\alpha / (\log X)^B} d^{3+\varepsilon},$$

and this is, by partial summation,

$$\ll X^{1/2+4\alpha+\varepsilon}.$$

For $\alpha < 1/8$, the sum in the assertion is

$$\ll X^{1/4+\varepsilon}$$

and clearly this is certainly $\ll \frac{X}{(\log X)^2}$. This proves the assertion. \square

Thus we can apply Theorem 4.5.1 to our situation and we will make this explicit now. To apply Theorem 4.5.1 we need to choose α, u, v, λ satisfying conditions of the theorem.

We choose as follows. We will take $k \geq 4$ and:

$$(6.1.4) \quad \alpha = \frac{1}{8} - \frac{1}{8k} = \frac{k-1}{8k},$$

$$(6.1.5) \quad u = \frac{8k}{k-1} + \frac{1}{k-1} = \frac{8k+1}{k-1}$$

$$(6.1.6) \quad v = \frac{4}{\alpha} = \frac{32k}{k-1},$$

$$(6.1.7) \quad \lambda = \frac{1}{\sqrt{\log(k)}}.$$

Then we have

$$\frac{1}{\alpha} = \frac{8k}{k-1} < u = \frac{8k+1}{k-1} < v = \frac{4}{\alpha} = \frac{32k}{k-1}.$$

With these choices, we define

$$G_3(k) = F\left(\frac{k-1}{8k}, \frac{32k}{k-1}, \frac{8k+1}{k-1}, \frac{1}{\sqrt{\log(k)}}\right)$$

explicitly this is given by

$$(6.1.8) \quad G_3(k) = \frac{e^\gamma}{32k\sqrt{\log(k)}} \left(8\log(3)k\sqrt{\log(k)} + \log(24k) - (1+8k)\log\left(\frac{32k}{1+8k}\right) \right)$$

and then it is clear that $G_3(k) > 0$ for $k \gg 0$ and numerically one checks that for $k \geq 3.609\dots$, we have $G_3(k) > 0$. Thus we have that $F(\alpha, v, u, \lambda) > 0$ for these choices of the parameters. So we can apply Theorem 4.5.1, and note that by the prime number theorem (or by Chebyshev's Theorem) we have $\#\mathcal{A} \gg \frac{X}{\log X}$ and so we deduce that

$$\mathcal{W}(\mathcal{A}, \mathcal{P}, u, v, \lambda) \gg \frac{X}{(\log X)^2}.$$

Now the rest of the proof proceeds mutatis mutandis along the lines of Theorem 2.2.2.

6.2. Now we can prove the corollary. For the Ramanujan modular form

$$\Delta(q) = \sum_{n=1}^{\infty} \tau(n)q^n$$

we have $k = 12$ and hence we deduce assuming GRH that, there exists infinitely many prime p such that

$$3 \leq \omega(p^{11} + 1 - \tau(p)) \leq [97 + \sqrt{\log(12)}] = 98.$$

As indicated in the introduction, the bound $\omega(N_p(\Delta)) \geq 3$ is a consequence of the Ramanujan congruences for $\Delta(q)$. This completes the proof of Theorem 2.2.3.

7. THE NORMAL ORDER OF $\omega(N_p(f))$

7.1. We show in this section that the average behavior of $\omega(N_p(f))$ is similar to the average behavior of $\omega(n)$. More precisely we have the following theorem.

Theorem 7.1.1. *Let f be a newform satisfying hypothesis of 2.1. Assume GRH. Then we have*

$$(7.1.2) \quad \lim_{X \rightarrow \infty} \frac{1}{\pi(X)} \# \left\{ p \leq X : \frac{\omega(N_p(f)) - \log \log(p)}{\sqrt{\log \log(p)}} \leq \gamma \right\} = G(\gamma),$$

where

$$G(\gamma) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\gamma} e^{-\frac{t^2}{2}} dt.$$

7.2. This will be proved by the method of proof of [Liu06, Theorem 1, page 156]. The proof of Theorem 7.1.1 is very similar to that of [Liu06, Theorem 1, page 156]. So we will only provide a brief sketch here. In [Liu06, Theorem 3, page 160] a general criterion is given for an arithmetic function to satisfy the Erdős-Kac theorem and this general result is applied to prove [Liu06, Theorem 1, page 156]. We show here that these criteria are also valid (under GRH) in the present case. We show that Theorem 7.1.1 is a consequence of the results of the previous sections and [Liu06, Theorem 3, page 160]. In this section we will use notations from [Liu06]. To apply [Liu06, Theorem 3, page 160] we have to verify the seven conditions (C) and (1)-(6) of loc.cit. are satisfied. In the interest of brevity we will not recall these here. But we will adhere to the notations of [Liu06]. We take the set $S = \{p \leq X : p \text{ a prime}\}$ and a function $N : S \rightarrow \mathbb{N}$ given by $p \mapsto N_p(f)$. Thus condition (C) is obviously satisfied and we note that by Lemma 3.6.3, the conditions (2), (4) and (5) hold (by GRH and Mertens's Theorem). Thus we have to verify condition (3) and (6). This needs the Chebotarev Theorem of [MMS88]. In the notation of [Liu06] we have

$$e_\ell = \frac{X^{1/2} \ell^3 \log(\ell^4 X)}{\pi(X)},$$

and so conditions (3) and (6) are verified exactly as in [Liu06] with $\beta < \frac{1}{10}$. This completes our sketch of Theorem 7.1.1.

8. EXAMPLES

We list examples of new forms of low level where the theorems apply. We summarize the data in a convenient form. Each row corresponds to a level. Each column corresponds to a weight. The (n, k) -th entry lists the number of distinct newforms satisfying hypothesis of 2.1. The ninety five forms in this list are all non-CM. The data provided here was extracted from the Modular Forms Database [Ste04] and also using Sage and PARI/GP software packages [Ste08, PAR08]. We note that the list is not exhaustive by any means. For instance, one can find forms of weights 48 on $\Gamma_0(2)$ and of weight 44 on $\Gamma_0(6)$ which satisfy hypothesis 2.1 (see [Unk]).

The empty spaces in the list are where our version of Sage failed to provide conclusive answers or the database did not return values.

| $N \downarrow, k \rightarrow$ | 4 | 6 | 8 | 10 | 12 | 14 | 16 | 18 | 20 | 22 | 24 | 26 |
|-------------------------------|---|---|---|----|----|----|----|----|----|----|----|----|
| 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 |
| 2 | 0 | 0 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 2 | 0 | 1 |
| 3 | 0 | 1 | 1 | 2 | 1 | | | | | | | |
| 4 | | | | | | | | | | | | |
| 5 | 1 | 1 | 1 | 1 | | | | | | | | |
| 6 | 1 | 1 | 1 | 1 | 3 | 1 | 3 | | | | | |
| 7 | 1 | 1 | 1 | | | | | | | | | |
| 8 | | | | | | | | | | | | |
| 9 | 0 | | | | | | | | | | | |
| 10 | 1 | 3 | 1 | 3 | 3 | | | | | | | |
| 11 | 0 | 1 | 0 | | | | | | | | | |
| 12 | | | | | | | | | | | | |
| 13 | 1 | 0 | 1 | | | | | | | | | |
| 14 | 2 | 2 | 2 | 2 | 2 | | | | | | | |
| 15 | 2 | 2 | 2 | 2 | 1 | | | | | | | |
| 16 | | | | | | | | | | | | |
| 17 | 1 | 2 | 1 | | | | | | | | | |
| 18 | | | | | | | | | | | | |
| 19 | 1 | 2 | | | | | | | | | | |
| 20 | | | | | | | | | | | | |
| 21 | 2 | 4 | 1 | 1 | 2 | | | | | | | |

9. REMARKS AND REFINEMENTS

9.1. Refined version of Koblitz' conjecture. Let f be a newform as in 2.1. Let ℓ be a prime and suppose that for all but finite number of primes p we have

$$\chi(p)p^{k-1} - a_p(f) + 1 \equiv 0 \pmod{\ell},$$

then we say that ℓ is an *almost Eisenstein prime for f* . Suppose $\nu(f)$ is the number of distinct almost Eisenstein primes for f . The number of such primes is finite by the Theorem [Rib85] (this is a subset of primes for which the mod ℓ Galois representation associated to f is reducible). Observe that $\omega(N_p(f)) \geq \nu(f)$ for all but finitely many p . Thus we are led to the following reformulation of Koblitz's conjecture:

Conjecture 9.1.1. Let f be a modular form as in 2.1. Let $\nu(f)$ denote number of almost Eisenstein primes for f . Then for $X \gg 0$ the number of primes $p \leq X$ such that $\omega(N_p(f)) = \nu(f) + 1$ is at least $\gg \frac{X}{\log(X)^2}$.

For example, for Δ , we have $\nu(\Delta) = 3$ and so the conjecture predicts that there are infinitely many primes p where $N_p(\Delta)$ has exactly four distinct prime factors. Here are all the primes $p \leq 16000$ with $\omega(N_p(\Delta)) = 4$.

| p | $N_p(\Delta)$ |
|-------|---|
| 5 | $2^{10} \cdot 3 \cdot 23 \cdot 691$ |
| 7 | $2^9 \cdot 3^5 \cdot 23 \cdot 691$ |
| 577 | $2^{13} \cdot 3^7 \cdot 691 \cdot 190641378938814930857$ |
| 1153 | $2^{13} \cdot 3^6 \cdot 691 \cdot 1160183970784175844330767$ |
| 1297 | $2^{11} \cdot 3^6 \cdot 691 \cdot 16935741217449799251621239$ |
| 3803 | $2^8 \cdot 3 \cdot 691 \cdot 4534718285139898177401117938327717$ |
| 5693 | $2^{10} \cdot 3 \cdot 691 \cdot 95907763393686429420185450510493683$ |
| 11317 | $2^{10} \cdot 3^5 \cdot 691 \cdot 2268089547548261526855554962441076239$ |
| 14437 | $2^{10} \cdot 3^6 \cdot 691 \cdot 11008825527208610156044088966777471773$ |
| 15307 | $2^8 \cdot 3 \cdot 5 \cdot 691 \cdot 251458672161512059369128893956312797721$ |

We remark that Conjecture 9.1.1 includes the following version of Koblitz's conjecture for elliptic curves. The original version of Koblitz' conjecture is made for elliptic curves which are not \mathbb{Q} -isogenous to an elliptic curve with torsion.

Conjecture 9.1.2. Let E/\mathbb{Q} be an elliptic curve. Let $t_E = \#E(\mathbb{Q})_{\text{tor}}$. Then for $X \gg 0$ the number of primes $p \leq X$ such that $\omega(N_p(E)) = \nu(t_E) + 1$ is at least $\gg \frac{X}{\log(X)^2}$.

Indeed, if q is a prime dividing the torsion subgroup of $E(\mathbb{Q})$, then it is well-known, that for primes p , of good reduction for E , we have $N_p(E) = p + 1 - a_p(E) \equiv 0 \pmod{q}$ (because torsion injects into the \mathbb{F}_p -rational points). Hence $\nu(N_p(E)) \geq \omega(t_E)$ and any prime q dividing t_E is an almost Eisenstein prime for E .

9.2. Ramanujan-Serre forms. In the introduction we indicated that the obvious variant Koblitz's question is false for $\Delta(q)$. Here we show that there exists infinitely many forms of weights k_i tending to infinity (as $i \rightarrow \infty$) such that for all primes p , we have $\omega(N_p(f_{k_i})) \geq 2$. The construction depends on what we should call *weak Ramanujan-Serre forms*. A *weak Ramanujan-Serre form* f for $\text{SL}_2(\mathbb{Z})$ is a normalized cusp (but not necessarily an eigen) form of weight k on $\text{SL}_2(\mathbb{Z})$ with coefficients in $\mathbb{Z}[1/N]$ for some $N \geq 1$ and which is congruent to the Eisenstein series of weight k for every prime q which divides the numerator of B_k/k . We say that a Hecke eigen form of weight k for $\text{SL}_2(\mathbb{Z})$ is a *strong Ramanujan-Serre form* if it is congruent to some weak Ramanujan-Serre form for every prime dividing B_k/k . The Ramanujan-Delta function is an example of this; so are the cusp forms of weights less than 24. The existence of such forms for low weights (the famous example being $\Delta(q)$) is due to Ramanujan. The existence of weak Ramanujan-Serre forms for all weights $k \geq 12$ is due to Serre (see [Rib77, Kha00]), so the name weak Ramanujan-Serre forms is appropriate; weak Ramanujan-Serre forms of weights ≤ 20 are also strong Ramanujan forms as there is only one prime dividing the corresponding B_k/k . The unique normalized cusp form $\Delta_{22}(q)$ of weight 22 is an example of a strong Ramanujan-Serre form (there are two primes 131 and 593 dividing $B_{22}/22$). Strong Ramanujan-Serre forms do not always exist. For instance there are no strong Ramanujan-Serre forms of weight $k = 24$. We do not know if strong Ramanujan-Serre forms always exist (for all weights). We recall that a conjecture of Honda asserts that there are no Hecke eigenforms for $\text{SL}_2(\mathbb{Z})$ satisfying $k \geq 28$ and with integer Fourier coefficients.

Remark 9.2.1. There exists an increasing, infinite sequence of integers $k_i \geq 12$ and weak Ramanujan-Serre forms f_{k_i} of weights k_i such that $\omega(N_p(f_{k_i})) \geq 2$. In particular $N_p(f_{k_i})$ are not primes for all primes p .

Proof. By a result of Serre [Rib77, Kha00], we are assured of the existence of weak Ramanujan-Serre forms. In other words there exists cusp form $f_k(q) = \sum_{n=1}^{\infty} a_n(f_k)q^n$ of weight k on $\mathrm{SL}_2(\mathbb{Z})$ with coefficients in $\mathbb{Z}[1/N]$ for some $N \geq 1$, such that for any prime ℓ dividing the numerator of B_k/k we have

$$E_k = -B_k/k + \sum_{n=1}^{\infty} \sigma_{k-1}(n)q^n \equiv f_k(q) \pmod{\ell}$$

and thus we deduce that $N_p(f_k) = p^{k-1} + 1 - a_p(f_k)$ has at least $\omega(B_k/k)$ prime divisors for $p \geq 2$. Thus we see that

$$\omega(B_k/k) \leq \omega(p^{k-1} + 1 - a_p(f_k)).$$

So it will suffice to prove that there is a sequence of k such that $\omega(B_k/k) \geq 2$.

To prove this we will use an old result of S. Chowla (see [Cho31]). It was shown in [Cho31] that if p is an odd prime such that p divides $\frac{B_n}{n}$ and such that p does not divide $2^n - 1$, then p divides the numerator of $B_{n+(p-1)i}$ for all $i \geq 0$. We choose $n = 24$ then $\frac{B_{24}}{24} = \frac{103 \cdot 2294797}{65520}$, while

$$2^{24} - 1 \not\equiv 0 \pmod{103},$$

so by Chowla's Theorem, we see that for any $i \geq 0$,

$$\frac{B_{24+102i}}{24+102i} \equiv 0 \pmod{103}.$$

Again for any $j \geq 0$, 691 divides the numerator of $\frac{B_{12+690j}}{12+690j}$. Since the arithmetic progressions $\{12+690j\}_j$ and $\{24+102i\}_i$ have infinitely many common elements (by the Chinese remainder theorem) so that we see that there exists an infinite number of integers $i \geq 0$ such that

$$\frac{B_{12+690i}}{12+690i} \equiv 0 \pmod{103 \cdot 691}.$$

Moreover, as $i \rightarrow \infty$ the numerator of $\frac{B_{12+690i}}{12+690i}$ goes to infinity as well and so $\omega(B_{12+690i}/(12+690i)) \geq 2$ as $i \rightarrow \infty$. Thus we may take $k_i = 12+690i$. Thus our assertion follows. \square

Remark 9.2.2. The existence of weak Serre-Ramanujan forms f_k as above has a curious consequence. In the notation of the above proposition we have $\omega(B_k/k) \leq \omega(2^{k-1} + 1 - a_2(f_k))$. Now for sufficiently large n , $\omega(n) \ll \frac{\log(n)}{\log(\log(n))}$. So we see that

$$\omega(B_k/k) \ll \frac{\log(2^{k-1} + 1 - a_2(f_k))}{\log \log(2^{k-1} + 1 - a_2(f_k))} \ll \frac{k}{\log(k)}.$$

So we have for $k \gg 0$,

$$\omega(B_k/k) \ll \frac{k}{\log(k)}.$$

We do not know a better upper bound for the number of prime factors of the numerator of B_k/k . We note that, as $\frac{B_k}{k} \asymp k^k$, the normal order heuristics would suggest $\omega(B_k/k) \asymp \log(k)$. But we do not know if B_k/k satisfies the normal order estimates.

REFERENCES

- [Bre01] Breuil, Christophe and Conrad, Brian and Diamond, Fred and Taylor, Richard, *On the modularity of elliptic curves over \mathbf{Q} : wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939.
- [Cho31] S. D. Chowla, *On a conjecture of Ramanujan*, Tohoku Math. J. **33** (1931), 1–2.
- [CM04] Alina Carmen Cojocaru and M. Ram Murty, *Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik’s problem*, Math. Ann. **330** (2004), no. 3, 601–625.
- [Coj05] Alina Carmen Cojocaru, *Reductions of an elliptic curve with almost prime orders*, Acta Arith. **119** (2005), no. 3, 265–289.
- [Del69] P. Deligne, *Formes modulaires et représentations ℓ -adiques*, Séminaire Bourbaki, 1968–1969, pp. 139–172.
- [HR74] H. Halberstam and H.-E. Richert, *Sieve methods*, Academic Press, 1974, London Mathematical Society Monographs, No. 4.
- [HW79] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, fifth ed., The Clarendon Press Oxford University Press, New York, 1979.
- [Kha00] Chandrashekhara Khare, *Notes on Ribet’s converse to Herbrand*, Cyclotomic fields and related topics (Pune, 1999), Bhaskaracharya Pratishthana, Pune, 2000, pp. 273–284.
- [Kob88] Neal Koblitz, *Primality of the number of points on an elliptic curve over a finite field*, Pacific J. Math. **131** (1988), no. 1, 157–165.
- [Liu06] Yu-Ru Liu, *Prime analogues of the Erdős-Kac theorem for elliptic curves*, J. Number Theory **119** (2006), no. 2, 155–170.
- [MM01] S. Ali Miri and V. Kumar Murty, *An application of sieve methods to elliptic curves*, Progress in cryptology—INDOCRYPT 2001 (Chennai), Lecture Notes in Comput. Sci., vol. 2247, Springer, Berlin, 2001, pp. 91–98.
- [MMS88] M. Ram Murty, V. Kumar Murty, and N. Saradha, *Modular forms and the Chebotarev density theorem*, Amer. J. Math. **110** (1988), no. 2, 253–281.
- [PAR08] PARI Group, Bordeaux, *PARI/GP, version 2.3.4*, 2008, available from <http://pari.math.u-bordeaux.fr/>.
- [Ram16] S. Ramanujan, *On certain arithmetical functions* [Trans. Cambridge Philos. Soc. **22** (1916), no. 9, 159–184], Collected papers of Srinivasa Ramanujan, AMS Chelsea Publ., Providence, RI, 2000, pp. 136–162.
- [Rib77] Kenneth A. Ribet, *Galois representations attached to eigenforms with Nebentypus*, Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), Springer, Berlin, 1977, pp. 17–51. Lecture Notes in Math., Vol. 601. MR MR0453647 (56 #11907)
- [Rib85] ———, *On l -adic representations attached to modular forms. II*, Glasgow Math. J. **27** (1985), 185–194. MR MR819838 (88a:11041)
- [Ser69] Jean-Pierre Serre, *Une interprétation des congruences relatives à la fonction τ de Ramanujan*, Séminaire Delange-Pisot-Poitou: 1967/68, Théorie des Nombres, Fasc. 1, Exp. 14, Secrétariat mathématique, Paris, 1969, p. 17.
- [Ser73] ———, *Congruences et formes modulaires [d’après H. P. F. Swinnerton-Dyer]*, Séminaire Bourbaki, 24e année (1971/1972), Exp. No. 416, Springer, Berlin, 1973, pp. 319–338. Lecture Notes in Math., Vol. 317.
- [Ste04] W. Stein, *The Modular Forms Database*, <http://modular.fas.harvard.edu/Tables> (2004).
- [Ste08] William Stein, *Sage: Open Source Mathematical Software (Version 2.10.2)*, The Sage Group, 2008, <http://www.sagemath.org>.
- [SW05a] Jörn Steuding and Annegret Weng, *On the number of prime divisors of the order of elliptic curves modulo p* , Acta Arith. **117** (2005), no. 4, 341–352.
- [SW05b] ———, *Erratum: “On the number of prime divisors of the order of elliptic curves modulo p ”* [Acta Arith. **117** (2005), no. 4, 341–352;], Acta Arith. **119** (2005), no. 4, 407–408.
- [Unk] Unknown, *Newforms with rational integer coefficients*, <http://www.lfunctions.org/degree2/degree2hm/integer.html>.
- [Was86] Lawrence C. Washington, *Some remarks on Cohen-Lenstra heuristics*, Math. Comp. **47** (1986), no. 176, 741–747.

MATH. DEPARTMENT, UNIVERSITY OF ARIZONA, 617 N SANTA RITA, TUCSON 85721-0089,
USA.

E-mail address: `kirti@math.arizona.edu`